



FIG. 2

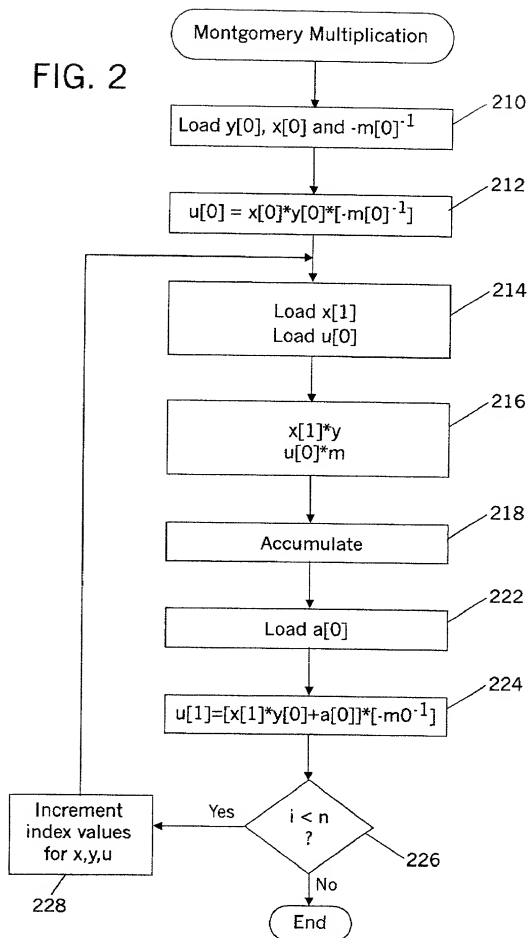
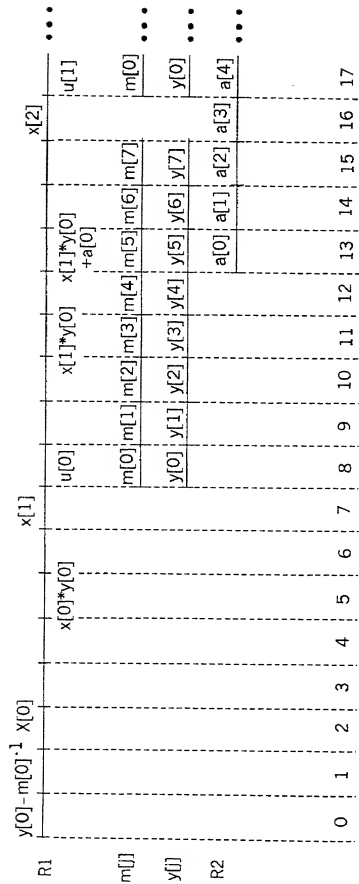


FIG. 3



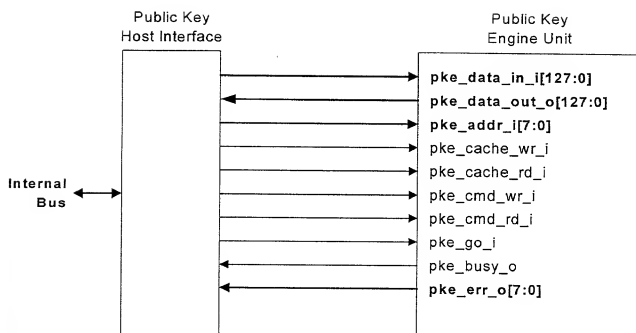


FIG. 4

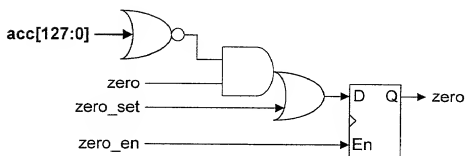


FIG. 12

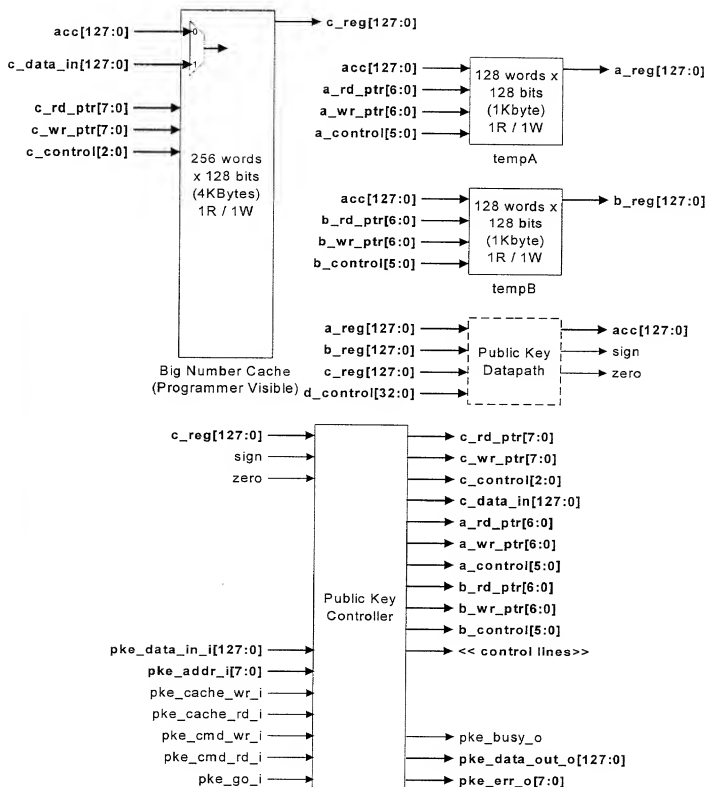


FIG. 5

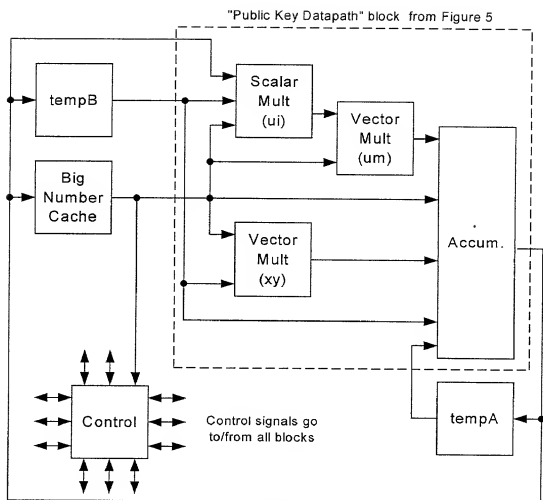


FIG. 6

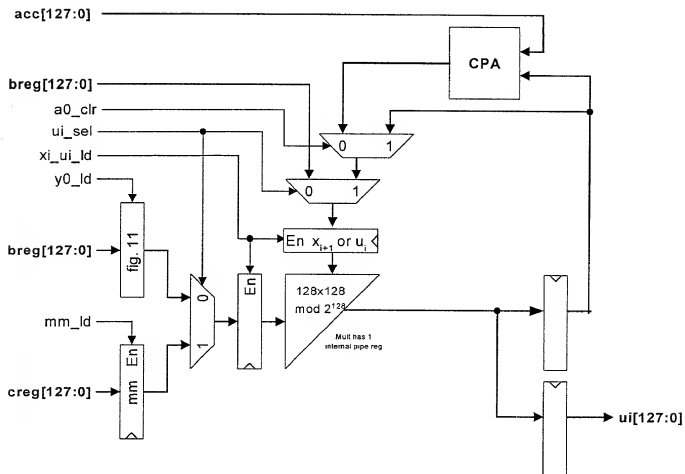


FIG. 7

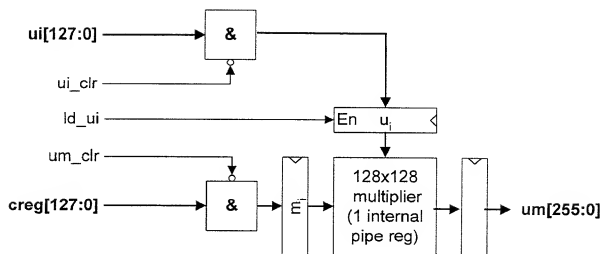


FIG. 8

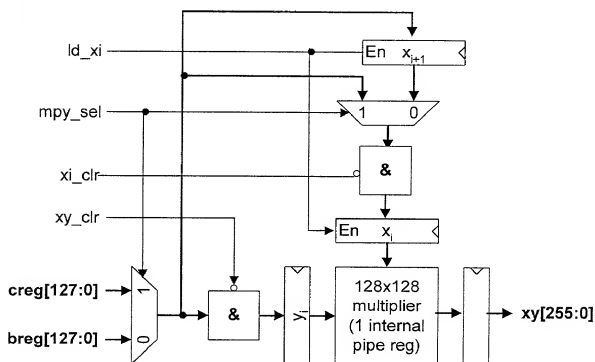


FIG. 9



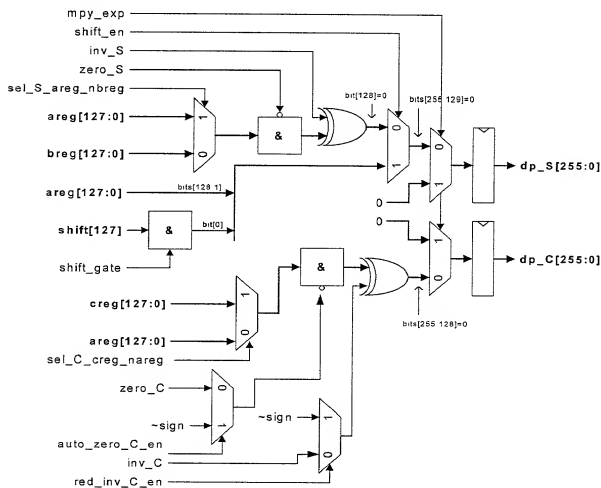
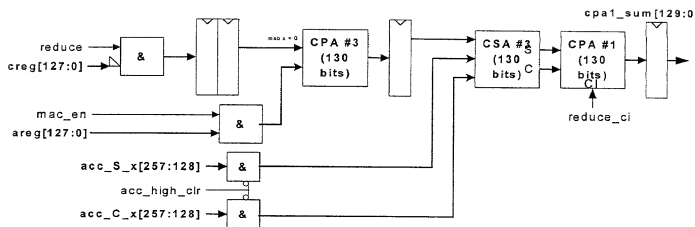


FIG. 10

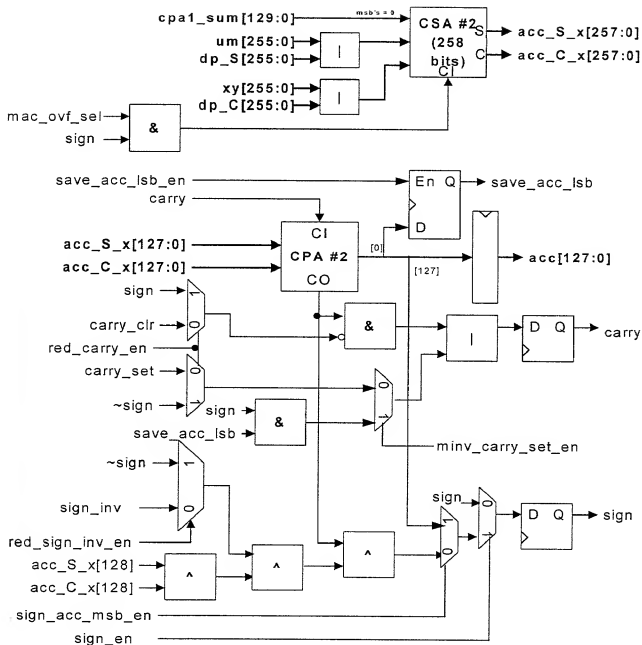


FIG. 11

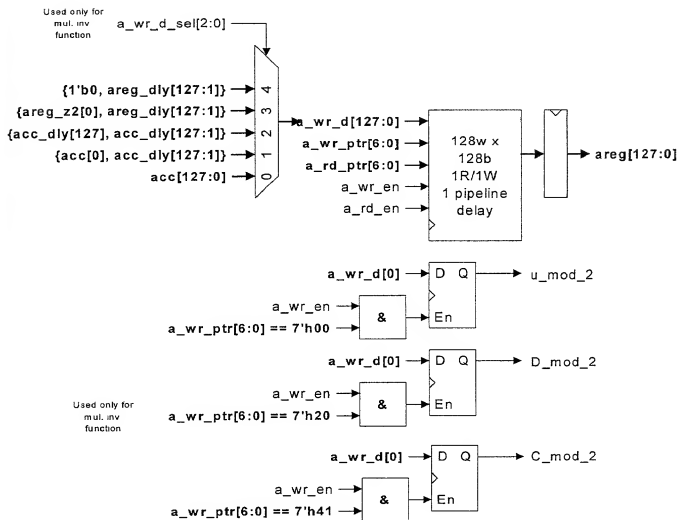
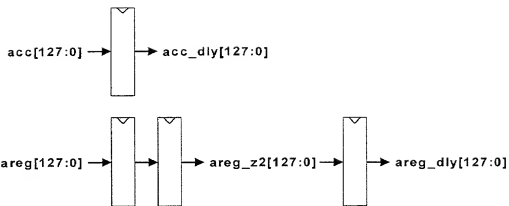


FIG. 13

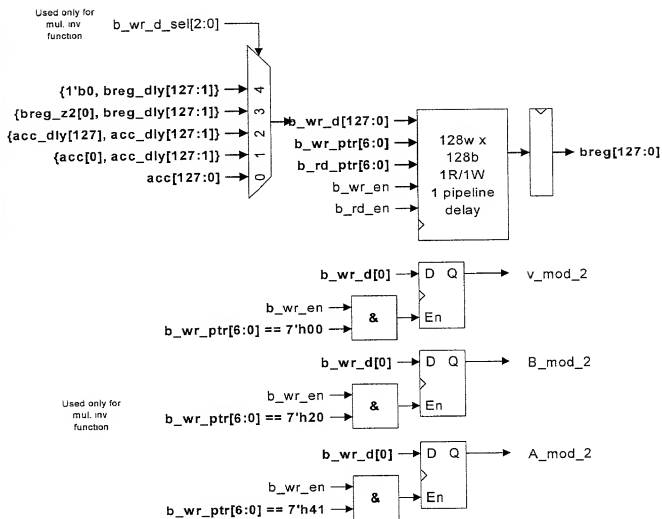
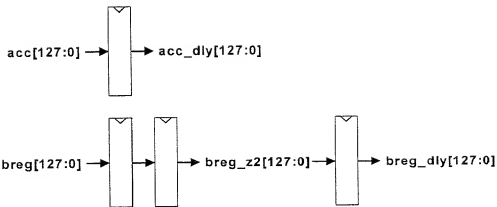


FIG. 14

FIG. 15

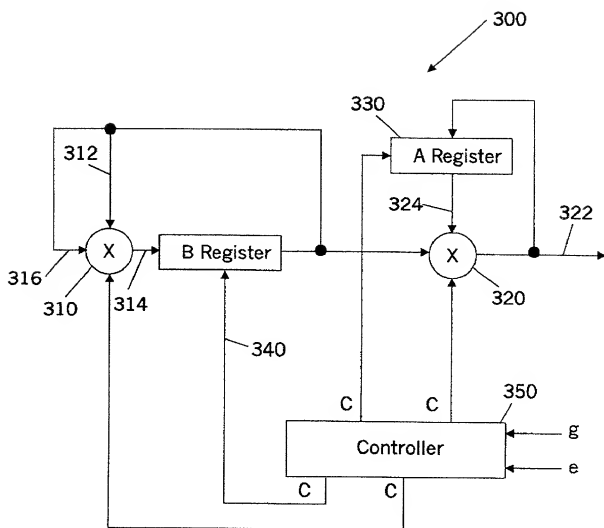


FIG. 16

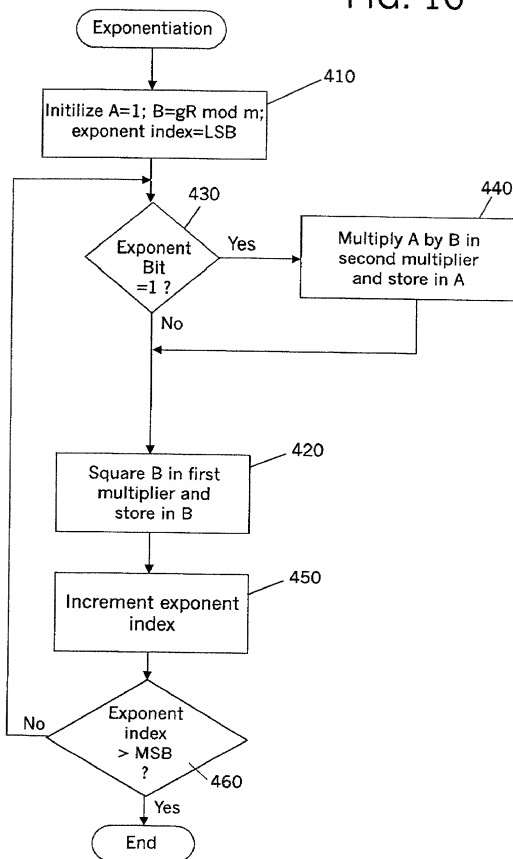


FIG. 17

Exponent Bit	LSB				MSB			
	0	1	1	0	1	0	0	1
A Register	1	$g^2 \bmod m$	$g^{2g^4} \bmod m$ $= g^6 \bmod m$	$g^6 \bmod m$	$g^{6g^{16}} \bmod m$ $= g^{22} \bmod m$	$g^{22} \bmod m$	$g^{22} \bmod m$	$g^{22g^{128}} \bmod m$ $= g^{150} \bmod m$
								...
B Register	$g^R \bmod m$	$g^{4R} \bmod m$	$g^{8R} \bmod m$	$g^{16R} \bmod m$	$g^{32R} \bmod m$	$g^{64R} \bmod m$	$g^{128R} \bmod m$	$g^{256R} \bmod m$
								...
Time	0	1	2	3	4	5	6	7
								8